Bloomberg Law® Privacy & Data Security

PRIVACY COMPLIANCE IN CLINICAL RESEARCH

Kristen B. Rosati[1] and Melissa A. Soliz[2]
Coppersmith Brockelman, PLC
http://www.cblawyers.com

OVERVIEW

This practical guidance document offers a broad overview of the privacy compliance issues regarding the use and disclosure of individually identifiable health information for human subjects research. It also contains a collection of checklists, sample forms, model contracting language, and template agreements.

Human subjects research includes scientific investigations that involve an experimental drug, device or biologic, or clinical interventions or interactions with a human subject volunteer (called a "Participant") that is intended to add to generalized medical knowledge.[3] Clinical trials are a subset of human subjects research that test an experimental drug, device or biologic, which are regulated by the Food and Drug Administration (the "FDA").[4] Clinical trials often are planned and funded by pharmaceutical or device companies, academic medical centers, federal agencies like the National Institutes of Health, or other

[1] Kristen Rosati is a Partner at Coppersmith Brockelman and a past President of the American Health Lawyer Association. Ms. Rosati serves on the planning committees for the AHLA Academic Medical Centers and Teaching Hospitals Institute. She also served on the planning committees for the 2017 AHLA Precision Medicine Institute and 2014 Annual Meeting of the International Society of Biomedical and Environmental Biorepositories. She is working with the Arizona Biomedical Research Commission to build clinical and translational research capacity in Arizona, including developing a "virtual" tissue bank. Ms. Rosati is also an advisor to the FDA Sentinel Initiative, a national distributed network to monitor medical product safety and efficacy, which is being leveraged for research purposes. She was a member of the Advisory Board for the Arizona State University (ASU) Biomedical Informatics Department and a founding Executive Committee member of the ASU Center for Health Care Innovation and Clinical Trials. Ms. Rosati is considered one of the nation's leading HIPAA compliance attorneys and has deep expertise with data sharing for research, biobanking, genomic privacy, and all matters related to "Big Data." Contact her via email at krosati@cblawyers.com.

[2] Melissa A. Soliz is an Associate at Coppersmith Brockelman. She is building a healthcare regulatory compliance practice that focuses on advising healthcare organizations on federal and state confidentiality laws (including 42 C.F.R. Part 2), breach reporting requirements, and data sharing for health information exchanges and research. Contact her via email at msoliz@cblawyers.com.

[3] *See* 45 C.F.R. § 164.501 ("*Research* means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."); 45 C.F.R. § 46.102(d) ("*Research* means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. . . .").

[4] 21 C.F.R. § 50.3(c) ("*Clinical investigation* means any experiment that involves a test article and one or more human subjects and that either is subject to requirements for prior submission to the Food and Drug Administration . . . ."); 21 C.F.R. § 50.3(j) ("*Test article* means any drug (including a biological product for human use), medical device for human use, human food additive, color additive, electronic product, or any other article subject to regulation under the act or under sections 351 and 354-360F of the Public Health Service Act (42 U.S.C. 262 and 263b-263n.").

organizations, which are referred to as the "Sponsor."[5] A physician or other professional who leads the implementation of a clinical trial at a research site is called the "Principal Investigator." The Principal Investigator will often be assisted by a research team of other doctors, nurses and health care professionals (collectively, "research personnel").[6] The research takes place at a physical site—*e.g.*, the hospital, clinic, or doctors' office, which is called a research site or "Institution."[7]

Three primary sets of federal regulations apply to clinical research: (1) the Health Information Portability and Accountability Act of 1996 and its implementing regulations (collectively, "HIPAA");[8] (2) the Common Rule;[9] and (3) the FDA Regulations.[10] In addition, other federal and state health confidentiality laws may impose more stringent protections on the use and disclosure of certain health information for research. Because HIPAA provides the most detailed privacy requirements for handling health information in clinical research, this paper provides detailed guidance on HIPAA's privacy protections. The paper briefly discusses the Common Rule, the FDA Regulations, and the potential application of other federal and state confidentiality requirements.

I. HIPAA PRIVACY RULE COMPLIANCE

HIPAA requires "Covered Entities"[11] to protect the privacy and security of Participants' protected health information ("PHI"), including when conducting clinical research.[12] Covered entities include most health care providers and all health plans.[13] The HIPAA Privacy Rule[14] restricts how Covered Entities may use and disclose PHI for purposes of clinical research. Generally, Covered Entities may only internally use (including use by employees and other agents) and externally disclose PHI to third parties, if one of the following requirements is satisfied:[15]

- The Participant or Participant's legally authorized representative ("LAR") signs a written HIPAA authorization;[16]
- An institutional review board ("IRB") waives or alters the HIPAA authorization requirement;[17]

5 *See generally* U.S. NAT'L INST. OF HEALTH, LEARN ABOUT CLINICAL TRIALS, https://clinicaltrials.gov/ct2/about-studies/learn (last visited Sept. 22, 2017).

6 *Id.*

7 *Id.*

8 Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended at 42 U.S.C. § 300gg, 29 U.S.C. § 1181 *et seq.* and 42 U.S.C. § 1320 *et seq.*; 45 C.F.R. Parts 146, 160, 162 and 164.

9 45 C.F.R. Part 46.

10 *See* 21 C.F.R. Parts 50 and 56. For a complete list of FDA regulations governing the conduct of clinical trials visit the FDA's website at: https://www.fda.gov/scienceresearch/specialtopics/runningclinicaltrials/ucm155713.htm.

11 45 C.F.R. §160.103 ("*Covered entity* means: (1) A health plan. (2) A health care clearing house. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.")

12 *See* 45 C.F.R. Part 164, Subpart E.

13 45 C.F.R. §160.103 (definition of "Covered Entity").

14 45 C.F.R. Part 160 and Subparts A and E of Part 164.

15 *See generally* NIH, RESEARCH REPOSITORIES, DATABASES AND THE HIPAA PRIVACY RULE 2 (Jan. 2004) [hereinafter "NIH PUB. 04-5489"], *available at* https://privacyruleandresearch.nih.gov/pdf/research_repositories_final.pdf.

16 45 C.F.R. § 164.508.

17 45 C.F.R. § 164.512(i).

- The activities are only to prepare for the clinical research, and the Principal Investigator makes certain representations;[18]
- The Institution and/or Principal Investigator are recruiting their own patients for the clinical research (or the patients of another health care provider under a business associate arrangement);[19]
- The PHI is de-identified;[20]
- Only a "Limited Data Set" is used and the Covered Entity enters into a "Data Use Agreement" with the recipient of the Limited Data Set;[21]
- The research involves the information of decedents only and the Principal Investigator makes certain representations;[22] or
- The research is "grandfathered" under the HIPAA rules.[23]

The following sections discuss the first six rules, as they are the most common situations raised in clinical research.

A. HIPAA Authorization

In most circumstances, the Principal Investigator will obtain a Participant's or LAR's written authorization to use and disclose the Participant's PHI for the clinical research.[24] A checklist that sets forth the required elements for a HIPAA-compliant authorization form for clinical research and sample HIPAA authorization for clinical research is included in Appendix.

Special consideration must be given if the PHI collected will be stored in a research repository for future research. HIPAA requires that the authorization adequately describe the storage and future research.[25] If the authorization for future use of the PHI will be combined with a HIPAA authorization to participate in a clinical trial (which involves treatment of the individual), then the authorization for future research must be structured as an "opt-in," separate from the authorization to participate in the clinical trial. That is because the HIPAA Privacy Rule prohibits "compound authorizations" where treatment can be conditioned on signing the HIPAA authorization form (such as in a clinical trial), with situations where treatment cannot be conditioned on signing the authorization form (such as the agreement to store PHI in a research repository for future research).[26]

B. IRB Waiver or Alteration of the HIPAA Authorization Requirement

Clinical research is reviewed by IRBs—ethics boards established to protect the rights and welfare of Participants. An IRB need not be owned by or affiliated with the research site, but the IRB (or a separate "privacy board") must be constituted as required by the regulations.[27] The IRB or privacy board can waive or alter the HIPAA authorization requirements by documenting its determinations that:

---

18 45 C.F.R. § 164.512(i).

19 45 C.F.R. § 164.506 (treatment or health care operations activities)

20 45 C.F.R. § 164.514(a)-(b).

21 45 C.F.R. § 164.514(c).

22 45 C.F.R. § 164.512(i).

23 45 C.F.R. § 164.512(i).

24 *See* 45 C.F.R. § 164.508(c) (HIPAA authorization form requirements).

25 OCR, RESEARCH (revised June 5, 2013) [hereinafter "OCR RESEARCH"], *available at* https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html.

26 45 C.F.R. § 164.508(b)(3); OCR RESEARCH, *supra*.

27 45 C.F.R. § 164.512(i)(1)(i).

- The use or disclosure involves no more than minimal risk to the privacy of the Participants based on the following factors:
    - An adequate plan to protect information identifying Participants from improper use and disclosure;
    - An adequate plan to destroy information identifying Participants at the earliest opportunity consistent with standard research conduct, unless there is a health or research justification for retention or if retention is required by law; and
    - Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the study, or for other research permitted by the HIPAA Privacy Rule;
- The clinical research could not practicably be conducted without the waiver or alteration of authorization; and
- The clinical research could not practicably be conducted without access to and use of the PHI.[28]

The IRB or privacy board must also include in its documentation:

- The date on which it approves an alteration or waiver of HIPAA authorization;
- A brief description of the PHI that may be used;
- A statement that the alteration or waiver has been reviewed and approved under either normal or expedited procedures; and
- The signature of the chair (or member designated by the chair) of the IRB.[29]

C. Activities to Prepare for Research

HIPAA authorization or IRB waiver is not required if the activities are limited to activities to prepare for research and the researchers make certain representations.[30] These activities typically take place before a research site or Principal Investigator participates in the research, such as developing a hypothesis, preparing a protocol, or determining whether there are sufficient numbers of patients in the site's records who would qualify to participate in a clinical research.[31] Contacting potential Participants to solicit their participation, however, is not a preparatory research activity. Participant recruitment is discussed in Section I.D below.

A Covered Entity may grant a researcher access to PHI for these preparatory activities if the researcher makes the following representations:

- The use or disclosure of PHI is sought solely to review PHI as necessary to prepare the clinical research protocol or similar preparatory purposes;
- No PHI is removed from the Covered Entity;[32] and
- The PHI is necessary for the clinical research.[33]

---

28 45 C.F.R. § 164.512(i)(2)(ii).

29 45 C.F.R. § 164.512(i)(2)(i), (iii)-(v).

30 45 C.F.R. § 164.512(i)(1)(ii).

31 NIH, CLINICAL RESEARCH AND THE HIPAA PRIVACY RULE 3-4 (Feb. 2004) [hereinafter "NIH PUB. 04-5495"], *available at* https://privacyruleandresearch.nih.gov/pdf/clin_research.pdf.

32 For guidance on remote access connectivity see NIH PUB. 03-5388, at 17, *supra*, and NIH, HEALTH SERVICES RESEARCH AND THE HIPAA PRIVACY RULE 14 (May 2005) [hereinafter "NIH PUB. 05-5308"], *available at* https://privacyruleandresearch.nih.gov/pdf/HealthServicesResearchHIPAAPrivacyRule.pdf.

33 45 C.F.R. § 164.512(i)(1)(ii); *see also* NIH PUB. 04-5495, at 3; NIH, Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule 17 (Apr. 2004) [hereinafter "NIH PUB. 03-5388"], *available at* https://privacyruleandresearch.nih.gov/pdf/HIPAA_Booklet_4-14-2003.pdf.

HIPAA permits research personnel to make these representations orally or in writing;[34] however, the best practice for Covered Entities is to obtain these representations in writing, signed by the research personnel.

D. Recruitment Activities

HIPAA authorization is not required if the Principal Investigator or research site is recruiting their own patients. This is permissible because HIPAA allows health care providers to contact their own patients about participating in clinical research because it is for "treatment" or "health care operations" purposes.[35] Covered Entities may also use a third party, such as a researcher, to recruit patients on behalf of the health care provider, as long as the Covered Entity gets a business associate agreement in place with the third party.[36] A template business associate agreement is included in the Appendix.

E. De-Identified Data

PHI that is de-identified before the use or disclosure for the research is not subject to HIPAA.[37] HIPAA provides two methods for de-identifying PHI: (1) removal or coding of all 18 HIPAA identifiers (referred to as the "safe harbor" method); or (2) statistical certification of de-identification (referred to as the "expert determination method").[38]

Under the safe harbor method, a Covered Entity either removes or codes the following 18 data elements about Participants and their family members, household members and employers:[39]

- Name;
- Street address, city, county, precinct, or zip code (unless only the first three digits of the zip code are used and the area has more than 20,000 residents);
- The month and day of dates directly related to an individual, such as birth date, admission date, discharge date, dates of service, or date of death;
- Age if over 89 (unless aggregated into a single category of age 90 and older);
- Telephone numbers;
- Fax numbers;
- Email addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers, serial numbers, and license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs) and Internet Protocol (IP) addresses;
- Biometric identifiers, such as fingerprints;

---

34 NIH PUB. 03-5388, at 17, *supra*.

35 45 C.F.R. § 164.506 (treatment or health care operations); NIH PUB. 04-5495, at 4, 9-10, *supra*.

36 NIH PUB. 04-5495, at 4, 9-10, *supra*.

37 45 C.F.R. § 164.502(d)(2); *see also* NIH PUB. 04-5489, at 3 ("The Privacy Rule permits covered entities to release data that have been de-identified without obtaining an Authorization and without further restrictions upon use or disclosure because de-identified data is not PHI and, therefore, not subject to the Privacy Rule.").

38 45 C.F.R. § 164.514(b).

39 45 C.F.R. § 164.514(b)(2)(i).

- Full-face photographs and any comparable images; and
- Any other unique identifying number, characteristic, or code.

If the Covered Entity knows that this de-identified information can still be used, either alone or in combination with other information, to identify Participants, then the information is still considered PHI and subject to HIPAA.[40] Moreover, if the information is coded,[41] disclosure of the code or other means to identify Participants is considered a disclosure of PHI and can only be disclosed pursuant to a HIPAA rule.[42]

Under the expert determination method for de-identifying data, a qualified statistician[43] using generally accepted statistical and scientific principles and methods determines that the risk is "very small" that the information, either alone or in combination with other reasonably available information, will identify Participants.[44] The statistician must document the method used and the results of the analysis to justify any determination that the information is statistically de-identified.[45] The Covered Entity must keep this documentation for at least six years.[46] An extensive guidance document regarding methods for de-identification of PHI is available on the HHS' website.[47]

De-identifying data is considered a "health care operations" activity and thus does not require patient authorization.[48] The Covered Entity may do the de-identification itself, or it can have a third party do so on its behalf, under a business associate agreement.[49] Once de-identified, the information may be used by a third party or the business associate.[50] However, the business associate may not retain the PHI after it's been de-identified, unless one of the other HIPAA rules applies.[51]

F. Limited Data Sets and Data Use Agreements

HIPAA permits Covered Entities to provide researchers and Sponsors with "Limited Data Sets" under a "Data Use Agreement" for use in clinical research.[52] Limited Data Sets are stripped of the "direct" HIPAA identifiers. Unlike fully de-identified information, a Limited Data Set may include:

---

40 45 C.F.R. § 164.514(b)(2)(ii).

41 A Covered Entity may use a code to mask the identifiers provided that: (a) the code is not derived from identifying information about the patient (e.g., a scrambled social security number, medical record number or name); and (b) the Covered Entity does not disclose the code. *See* 45 C.F.R. § 164.514(c). *See also* NIH Pub. 04-5489, at 8-9, 10, *supra*. "[A] randomly assigned re-identification code would not make the de-identified information to which it is assigned PHI, because a random code would not be derived from or related to information about the individual." *Id.*, at 6.

42 45 C.F.R. § 164.502(d)(2).

43 HIPAA requires that the person have "appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable." 45 C.F.R. § 164.514(b)(1).

44 45 C.F.R. § 164.514(b)(1)(i).

45 45 C.F.R. § 164.514(b)(1)(ii).

46 45 C.F.R. § 164.530(j)(2).

47 OCR, GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INFORMATION PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE (Nov. 2012), *available at* https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.

48 45 C.F.R. §§ 164.501 (defining health care operations), 164.506.

49 45 C.F.R. § 164.502(d)(1); NIH PUB. 03-5388, at 10, *supra*. A template business associate agreement that can be used for this purpose is included in the Appendix.

50 45 C.F.R. § 164.502(d)(1).

51 45 C.F.R. §§ 164.502(e), 164.504(e).

52 45 C.F.R. § 164.514(e)(3)

- Geographic designations above the street level or PO Box (such as a city or zip code);
- Dates directly related to a Participant (such as dates of service, birth dates, admission dates, discharge dates, or dates of death); and
- Any other unique identifying number, characteristic, or code that is not expressly listed as an "identifier."[53]

The Data Use Agreement must include the following:

- The permitted uses and disclosures of the Limited Data Set by the recipient. The recipient cannot use or disclose the Limited Data Set in a manner that would violate the HIPAA Privacy Rule if done by the Covered Entity;
- Who is permitted to use or receive the Limited Data Set (*e.g.*, list the names of the researchers);
- A requirement that the recipient will not use or further disclose the information in the Limited Data Set other than as permitted in the agreement or required by law;
- A requirement that the recipient will use appropriate safeguards to prevent unauthorized uses or disclosures;
- A requirement that the recipient must report to the Covered Entity any unauthorized use or disclosure of the information in the Limited Data Set of which it becomes aware;
- Assurances that any agents to whom the recipient provides the Limited Data Set agree to the same restrictions and conditions that apply to recipient with respect to that information; and
- A prohibition on identifying the information or contacting the Participants.[54]

Model language for a template Data Use Agreement is included in the Appendix.

Covered Entities that disclose Limited Data Sets under a Data Use Agreement are not required to also enter into a business associate agreement with the recipient.[55] However, a business associate agreement is required if the recipient is also the entity that will create the Limited Data Set for the Covered Entity.[56]

II. THE REVISED COMMON RULES

The "Common Rule" is the set of regulations that governs federally-funded or federally-conducted human subjects research. It is called the "Common Rule," because multiple federal agencies have adopted the same set of regulations.[57] Unlike HIPAA, the Common Rule does not provide prescriptive rules on how to protect the privacy of Participants. Instead, it requires an IRB to minimize risk to Participants, and requires the informed consent to include a statement describing how confidentiality of records identifying the Participant will be maintained.[58]

---

[53] 45 C.F.R. § 164.514(e)(2) ("A limited data set is protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State, and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images."); *see also* NIH Pub. 04-5489, at 3-4, *supra*.

[54] 45 C.F.R. § 164.514(e)(4).

[55] 45 C.F.R. § 164.504(e)(3)(iv).

[56] NIH PUB. 04-5495, at 13-14, *supra*. A template business associate agreement that can be used for this purpose is included in the Appendix.

[57] *See, e.g.,* 45 C.F.R. Part 46 (regulations applying to HHS-funded or conducted research).

[58] 45 C.F.R. §§ 46.111 and 46.116.

On January 19, 2017, the federal agencies that follow the Common Rule (including HHS) published a final rule revising the regulations.[59] The majority of revisions are effective January 19, 2018.[60] One significant revision is the new HIPAA exemption to the Common Rule. Under this new exemption, secondary research with identifiable information will be exempt from the Common Rule, so long as the research is regulated by HIPAA (*i.e.*, the PHI stays within the Covered Entity or is transferred to another HIPAA Covered Entity or business associate).[61] The exemption does not apply if the PHI is disclosed to an entity that is not regulated by HIPAA, such as a commercial Sponsor.

The revised Common Rule also has two new exemptions for storage and secondary use of identifiable information, where the information was collected for clinical purposes or for research studies other than the proposed research.[62] The new exemptions both require limited IRB review and "broad consent."[63]

III. FDA REGULATIONS

The FDA regulations at 21 C.F.R. Parts 50 and 56 replicate many of the Common Rule's human subject protections. The FDA regulations apply only to clinical investigations (clinical trials).[64]

IV. OTHER PRIVACY COMPLIANCE CONSIDERATIONS

Researchers must also consider whether other federal and state health confidentiality laws will impose more privacy protection than HIPAA. Whether other laws apply depends on (1) whether sensitive types of health information are involved (*e.g.*, substance use disorder treatment information, genetic information, HIV/AIDS), (2) who is the source of the health information (*e.g.*, a federally-assisted substance use disorder treatment program), and (3) who will have access to the covered health information for research purposes.

For example, if the clinical research will involve Participants who receive substance use disorder treatment from federally-assisted substance use disorder treatment programs, then the federal Confidentiality of Substance Use Disorder Patient Records regulations (42 C.F.R. Part 2) might apply if the health information used and disclosed identify a Participant as a substance abuser (called "Part 2

59 82 Fed. Reg. 7149 (Jan. 19, 2017).

60 82 Fed. Reg. at 7149, *supra*.

61 82 Fed. Reg. at 7262 (§ ____.104(d)(4)(iii)) ("Except as described in paragraph (a) of this section, the following categories of human subjects research are exempt from this policy: . . . (4) Secondary research. The research involves only information collection and analysis involving the investigator's use of identifiable health information when that use is regulated under 45 CFR parts 160 and 164, subparts A and E, for the purposes of 'health care operations' or 'research' as those terms are defined at 45 CFR 164.501 or for 'public health activities and purposes' as described under 45 CFR 164.512(b) . . . ."); *id.* at 7194 ("HIPAA also provides protections in the research context for the information that would be subject to this exemption (e.g., clinical records), such that additional Common Rule requirements for consent should be unnecessary in those contexts. Under HIPAA, these protections include, where appropriate, requirements to obtain the individual's authorization for future, secondary research uses of protected health information, or waiver of that authorization by an IRB or HIPAA Privacy Board. This provision introduces a clearer distinction between when the Common Rule and the HIPAA Privacy Rule apply to research in order to avoid duplication of regulatory burden. We believe that the HIPAA protections are adequate for this type of research, and that it is unduly burdensome and confusing to require applying the protections of both HIPAA and an additional set of protections").

62 82 Fed. Reg. at 7194.

63 82 Fed. Reg. at 7261-62, 7264 (Final Rule §§ __.104(d)(8)(i)-(iii), __.111(a)(7)).

64 21 C.F.R. § 56.101 ("This part contains the general standards for the composition, operation, and responsibility of an Institutional Review Board (IRB) that reviews clinical investigations regulated by the Food and Drug Administration under sections 505(i) [exemption for new drugs for investigational use] and 520(g) [exemption for devices for investigational use] of the act, as well as clinical investigations that support applications for research or marketing permits for products regulated by the Food and Drug Administration . . . ."); *id.* § 50.1(a) (stating same).

information").[65] The Part 2 regulations impose unique patient consent requirements on the use and disclosure of Part 2 information, and have different rules when Part 2 information may be used for research without patient consent.[66]

State laws might also more stringently protect the use and disclosure of other categories of sensitive health information, such as genetic information, communicable disease-related information, HIV/AIDS, mental health or substance abuse; state laws may also have more stringent laws that apply to all health information. For example, state law might require an authorization form for research to expressly permit the disclosure of HIV/AIDS-related information.[67] Researchers should be familiar with the state laws of the patients who will be Participants in the clinical research.

APPENDIX: PRACTICAL GUIDANCE MATERIALS

To assist readers in complying with HIPAA, the authors have complied the following practical guidance materials: a HIPAA authorization checklist for clinical research; a sample HIPAA authorization form for clinical research; model contracting language (including clinical trial agreement privacy requirements and data use agreement language); and a template business associate agreement.

65 42 C.F.R. § 2.12(a).

66 42 C.F.R. § 2.31.

67 *See, e.g.*, A.R.S. § 36-664(F).

HIPAA AUTHORIZATION CHECKLIST FOR CLINICAL RESEARCH

A HIPAA-compliant authorization form used for clinical research must include the following:

- √ A specific and meaningful description of the PHI to be used or disclosed (*e.g.*, the Participant's medical records or limited portions of the record, such as laboratory results).
- √ The name or specific identification of the persons or class of persons authorized to make the disclosure (*e.g.*, the Participant's physicians and treating hospitals).
- √ The name or specific identification of the persons or class of persons who will have access to the PHI (*e.g.*, Principal Investigator, Study Site, IRB, FDA, and HHS).
- √ A description of the research protocol or study. If PHI will be stored in a research repository or otherwise will be used in future research, the authorization must clearly describe that storage/use.
- √ A statement that the Participant will not be permitted to participate in the clinical research if he or she does not sign the authorization. However, if the PHI will be used for research unrelated to the particular clinical trial (such as storage in a data repository to use for future research), the authorization form must have a separate "opt-in" for that purpose, and the entity may not require a Participant to sign that portion of the HIPAA authorization. If the informed consent document requires the Participant to agree to use of PHI for future research, the HIPAA authorization may not be combined with the informed consent document.
- √ An expiration date or event (such as the end of the study), or a statement that the authorization has no expiration.
- √ A statement of the Participant's right to revoke the authorization in writing and a description of how to do so.
- √ A statement that the Participant may not revoke the authorization as to information already disclosed for the research where the information is necessary to maintain the integrity of the study data (or a description of other exceptions where the Participant may not revoke the authorization).
- √ A statement that the information disclosed for the clinical research may be subject to redisclosure by the recipient and no longer be protected by the federal privacy rule.
- √ If the Participant will not be given access to medical records during the clinical research, a statement that the Participant agrees to the denial of access and that the right to access medical records will be reinstated upon completion of the clinical research.
- √ If the Covered Entity will receive direct or indirect remuneration for the individual's PHI (versus the clinical research services), and the remuneration is not capped at the Covered Entity's cost to prepare and transmit the PHI, a statement that the Institution is receiving payment for the PHI.
- √ The Participant's signature and the date of signature.
- √ If the authorization is executed by a personal representative of the Participant (the Participant's LAR), a description of that person's authority to act for the Participant.

SAMPLE HIPAA AUTHORIZATION FOR CLINICAL RESEARCH

Participant's Name: _____

Research Study: *[Insert name of Protocol]*

Sponsor: *[Insert name of Sponsor]*

Principal Investigator: *[Insert name of PI]*

Research Site(s): *[Insert legal name and dba of each facility and /or physician office that is a site for the study]*

You have been asked to participate in this Research Study. If you sign this Authorization Form, you agree to the use and disclosure (release) of your health information for the Research Study, as described in this Authorization Form.

The following health information about you may be collected for this Research Study: *[insert complete description of the information that will be collected about research participants in the study]*.

Your health information may be used for this Research Study by each Research Site, the Principal Investigator, and their representatives. Your health information may also be disclosed by each Research Site, the Principal Investigator and your other health care providers to the following people and organizations: the affiliates of the Research Site and the Principal Investigator; the Sponsor and its representatives; government agencies in the United States that regulate clinical research, including the Food and Drug Administration (FDA) and the Office for Human Research Protections; government agencies in foreign countries that regulate clinical research; the Institutional Review Board that is responsible for reviewing the Research Study; *[insert any other organization that will see health information about the participants, such as a CRO or a data safety monitoring board]*.

The people who see your health information for this Research Study might not be required to follow the federal privacy law (called HIPAA). They might share your information with others without your permission if they are permitted to do so by other laws that apply to them.

If you do not sign this form, you cannot be in the Research Study. If you do not sign this form, it will not affect your treatment, the payment for that treatment, or enrollment or eligibility for benefits.

[Optional – insert if a research participant in the particular study will not be able to review medical records related to the study: You will not be able to see your health information related to the Research Study until the Research Study is complete. At the end of the Research Study, you may ask for access to your health information, as described in the Research Site's Notice of Privacy Practices.]

You may change your mind and revoke (take back) this Authorization Form at any time, unless your health information was already disclosed based on this Authorization Form or unless it is necessary to continue using your health information to maintain the integrity of the Research Study. To revoke this Authorization, you must write to: *[Insert name or title and insert address]*. This Authorization will not expire unless you revoke it.

_____ _____

Signature Date

_____

Printed Name

_____

* If this is signed by an authorized personal representative of the participant, indicate the representative's relationship to the participant or authority to act on behalf of the participant.

MODEL CONTRACTING LANGUAGE FOR HIPAA COMPLIANCE

I. USE OF PHI IN A CLINICAL TRIAL AGREEMENT

This model contracting language for HIPAA compliance can be incorporated into a clinical trial agreement ("CTA"). A CTA sets forth the contractual and compliance obligations between the Sponsor, the research site (the Institution), and Principal Investigator.

Each Party will comply with all applicable laws and regulations relating to privacy and security of protected health information ("PHI"), including the Health Information Insurance Portability and Accountability Act of 1996 and its implementing regulations (collectively, "HIPAA").

Sponsor shall have the right to review and approve the HIPAA authorization and informed consent document, including any subsequent modifications thereto. Principal Investigator will obtain from each Participant at the time of enrollment a signed HIPAA authorization and informed consent document that have been approved by the IRB and Sponsor.

Sponsor will not use PHI received from Institution and will not disclose PHI to any third party except: (a) as permitted by the Participant's informed consent document; (b) when required by law, regulation, or government order; or (c) pursuant to the Participant's written request. If Sponsor contracts with any agents to whom it provides a Participant's PHI, it will include provisions in those agreements through which its agents agree to the same restrictions and conditions that apply to Sponsor regarding PHI.

II. DATA USE AGREEMENT

This Data Use Agreement language is required for disclosure of a Limited Data Set. It can be a free-standing agreement, or a separate section in a CTA. This model language refers to "Recipient," which might be a Sponsor or other organization that receives the Limited Data Set for research.

1. Uses and Disclosures of Limited Data Set. Recipient will use and disclose the Limited Data Set only for those purposes necessary to perform research functions in the *[insert the name of the clinical trial (the "Study")]*, or as required by law. Recipient will not otherwise use or further disclose any information included in the Limited Data Set.

2. Designation of Personnel. Recipient designates the following personnel as individuals who will receive, use and disclose the Limited Data Set on Recipient's behalf ("Personnel"): *[Insert either specific individuals or categories of individuals by role]*.

Recipient will require Personnel to comply with the terms of this Data Use Agreement. Recipient represents and warrants that Personnel are under legal obligation to Sponsor, by contract or otherwise, to comply with Recipient's instructions to comply with this Data Use Agreement.

3. Safeguards. Recipient will implement appropriate safeguards to prevent any use or disclosure of the Limited Data Set not otherwise permitted in this Agreement.

4. Reports of Impermissible Use or Disclosure. Recipient will report to Institution any use or disclosure of the Limited Data Set not permitted by this Data use Agreement within *[insert time period – five (5) business days is recommended]* business days of Recipient learning of such use or disclosure.

5. Agents and Subcontractors. If Recipient provides the Limited Data Set to an agent or subcontractor for a purpose authorized under this Agreement, Recipient first will enter into a written contract with the agent or subcontractor that requires the agent or subcontractor to agree to the same restrictions and conditions as contained in this Data Use Agreement.

6. Prohibition on Identifying and Contacting Individuals. Recipient agrees that it will not attempt to learn the identity of the individuals represented in the Limited Data Set. If Recipient does learn the identity of the individuals, it agrees not to contact those individuals.

MODEL BUSINESS ASSOCIATE AGREEMENT

This template agreement can be used when a Covered Entity engages a third party, such as a non-employed Principal Investigator or other researcher, to de-identify PHI or create a Limited Data Set for use in clinical research. It can also be used if a third party will be recruiting a Covered Entity's patients on behalf of the Covered Entity for participation in clinical research.

This Business Associate Agreement ("BAA") is entered into between *[insert name]* ("Covered Entity") and *[insert name]* ("Business Associate"), with an effective date of *[insert date]* ("Effective Date"). This BAA sets out the responsibilities and obligations of Business Associate as a business associate of Covered Entity under the Health Insurance Portability and Accountability Act and its implementing regulations (collectively, "HIPAA"). Covered Entity and Company are each a "Party" and the "Parties" to this BAA.

RECITALS

Covered Entity has engaged Business Associate *[insert "to provide de-identification services in accordance with 45 C.F.R. § 164.514(b)"; "to create a limited data set in accordance with 45 C.F.R. § 164.514(e)"; or "to contact the Covered Entity's patients about participation in clinical research"]* ("Services").

Covered Entity may make available to Business Associate Protected Health Information ("PHI") of Individuals in conjunction with Services, which Business Associate will Use or Disclose only in accordance with this BAA.

NOW THEREFORE, for good and valuable consideration, the Parties, intending to be legally bound, hereby agree as follows:

AGREEMENT

Business Associate and Covered Entity agree to the terms and conditions of this BAA in order to comply with the rules on handling of PHI under the HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E ("Privacy Rule"), the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C ("Security Rule"), and the HIPAA Breach Notification Regulations, 45 C.F.R. Part 164, Subpart D ("Breach Notification Rule"), all as amended from time to time.

1. DEFINITIONS

a. Terms Defined in Regulation: Unless otherwise provided in this BAA, all capitalized terms in this BAA will have the same meaning as provided under the Privacy Rule, the Security Rule and the Breach Notification Rule.

b. Protected Health Information or PHI: Protected Health Information ("PHI") means PHI that Business Associate receives from Covered Entity, or creates, maintains or transmits on behalf of Covered Entity.

2. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

a. Performance of Services: Business Associate will Use or Disclose PHI only for those purposes necessary to perform Services, or as otherwise expressly permitted in this BAA or required by law, and will not further Use or Disclose such PHI.

b. De-Identification: Business Associate will de-identify PHI in accordance with 45 C.F.R. § 164.514 and may use or disclose such de-identified data. *[NOTE FOR DRAFTING: Covered Entity could chose to place contractual restrictions on the Business Associate's use and disclosure of the de-identified data. For example, Covered Entity could provide that Business Associate may only use or disclose de-identified data to provider Services; the regulations do not require that restriction]*

c. Limited Data Sets: Business Associate will Use the PHI to create a Limited Data Set in accordance with 45 C.F.R. § 164.514(e). Business Associate will not Use the Limited Data Set for its own purposes and will not Disclose the Limited Data Set to any person or entity other than Covered Entity. *[NOTE FOR DRAFTING: If Business Associate will also be a recipient of the Limited Data Set, Business Associate must also enter into a Data Use Agreement with Covered Entity or incorporate the required content of a Data Use Agreement into this the BAA.]*

d. Recruitment: Business Associate will Use the PHI to contact Covered Entity's patients to discuss participation in clinical research. *[NOTE FOR DRAFTING: This section can support business associate recruitment activities across clinical trials, or can be restricted to a particular clinical trial. Many Covered Entities will want to exercise control over a business associate's contact with their patients, and thus will add detail to this section.]*

e. Subcontractors: Business Associate agrees that, in accordance with § 164.502(e)(1), if Business Associate's Subcontractor creates, receives, maintains or transmits PHI on behalf of Business Associate, Business Associate will enter into an agreement with such Subcontractor that contains the same restrictions and conditions on the Use and Disclosure of PHI as contained in this BAA.

f. Business Associate Management, Administration and Legal Responsibilities: Business Associate may Use PHI for Business Associate's management and administration, or to carry out Business Associate's legal responsibilities. Business Associate may Disclose PHI to a third party for such purposes only if: (1) the Disclosure is required by law; or (2) Business Associate secures written assurance from the receiving party that the receiving party will: (i) hold the PHI confidentially; (ii) Use or Disclose the PHI only as required by law or for the purposes for which it was Disclosed to the recipient; and (iii) notify the Business Associate of any other Use or Disclosure of PHI. *[NOTE FOR DRAFTING: This provision is not required by the regulations, but a Business Associate cannot use or disclose PHI for these purposes unless this is in the agreement.]*

g. Data Aggregation: Business Associate may Use PHI to perform data aggregation services as permitted by 45 C.F.R. § 164.504(e)(2)(i)(B). *[NOTE FOR DRAFTING: This provision is not required by the regulations, but a Business Associate may not use PHI for data aggregation unless permitted to do so by the BAA.]*

h. Covered Entity Responsibilities: To the extent Business Associate is to carry out Covered Entity's obligations under the Privacy Rule, Business Associate will comply with the requirements of the Privacy Rule that apply to Covered Entity's compliance with such obligations.

3. SAFEGUARDS FOR PROTECTED HEALTH INFORMATION

a. Adequate Safeguards: Business Associate will implement and maintain appropriate safeguards to prevent any Use or Disclosure of PHI for purposes other than those permitted by this BAA, including administrative, physical and technical safeguards to protect the confidentiality, integrity, and availability of any Electronic Protected Health Information ("ePHI"), if any, that Business Associate creates, receives, maintains, and transmits on behalf of Covered Entity.

b. Compliance with HIPAA Security Rule: Business Associate will comply with the applicable requirements of the HIPAA Security Rule.

4. REPORTS OF IMPROPER USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION, SECURITY INCIDENTS AND BREACHES

a. Use or Disclosure Not Permitted by This BAA: Business Associate will report in writing to Covered Entity any Use or Disclosure of PHI for purposes other than those permitted by this BAA within five (5) business days of Business Associate's learning of such Use or Disclosure. *[NOTE FOR DRAFTING: The timeline for reporting is negotiable. Most business associates will ask for a longer period of time.]*

b. Security Incidents: Business Associate will report in writing to Covered Entity any Security Incident of which Business Associate becomes aware. Specifically, Business Associate will report to Covered Entity any successful unauthorized access, Use, Disclosure, modification, or destruction of ePHI or interference with system operations in an information system containing ePHI of which Business Associate becomes aware within five (5) business days of Business Associate learning of such Security Incident. Notwithstanding the foregoing, Business Associate and Covered Entity acknowledge the ongoing existence and occurrence of attempted but unsuccessful Security Incidents that are trivial in nature, such as pings and port scans, and Covered Entity acknowledges and agrees that no additional notification to Covered Entity of such unsuccessful Security Incidents is required. However, to the extent that Business Associate becomes aware of an unusually high number of such unsuccessful Security Incidents due to the repeated acts of a single party, Business Associate shall notify Covered Entity of these attempts and provide the name, if available, of said party. *[NOTE FOR DRAFTING: The timeline for reporting is*

negotiable. The treatment of unsuccessful Security Incidents is negotiable, as long as some reporting upon request is included.]

c. Breaches of Unsecured PHI: Business Associate will report in writing to Covered Entity any Breach of Unsecured Protected Health Information, as defined in the Breach Notification Rule, within five (5) business days of the date Business Associate learns of the incident giving rise to the Breach. Business Associate will provide such information to Covered Entity as required in the Breach Notification Rule. *[NOTE FOR DRAFTING: The timeline for reporting is negotiable. HIPAA requires a business associate to report "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach." Most business associates will ask for a longer period of time.]*

5. ACCESS TO PROTECTED HEALTH INFORMATION

a. Covered Entity Access: Within five (5) business days of a request by Covered Entity for access to PHI, Business Associate will make requested PHI available to Covered Entity.

b. Individual Access: If an Individual makes a request for access directly to Business Associate, Business Associate will within five (5) business days forward such request in writing to Covered Entity. Covered Entity will be responsible for making all determinations regarding the grant or denial of an Individual's request for PHI and Business Associate will make no such determinations. Only Covered Entity will release PHI to an Individual pursuant to such a request, unless Covered Entity directs Business Associate to do so. *[NOTE FOR DRAFTING: The timelines in both provisions are negotiable. Covered Entity must respond to an individual request for access within 30 days.]*

6. AMENDMENT OF PROTECTED HEALTH INFORMATION

a. Covered Entity Request: Within five (5) business days of receiving a request from Covered Entity to amend an Individual's PHI, Business Associate will provide such PHI to Covered Entity for amendment. Alternatively, if Covered Entity's request includes specific instructions on how to amend the PHI, Business Associate will incorporate such amendment into the PHI it holds in a Designated Record Set within five (5) business days of receipt of the Covered Entity request.

b. Individual Request: If an Individual makes a request for amendment directly to Business Associate, Business Associate will within five (5) business days forward such request in writing to Covered Entity. Covered Entity will be responsible for making all determinations regarding amendments to PHI and Business Associate will make no such determinations unless Covered Entity directs Business Associate to do so. *[NOTE FOR DRAFTING: The timelines in both provisions are negotiable. Covered Entity must respond to an individual request for amendment within 60 days.]*

7. ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

a. Disclosure Records: Business Associate will keep a record of any Disclosure of PHI that Business Associate makes, if Covered Entity would be required to provide an accounting to Individuals of such Disclosures under 45 C.F.R. § 164.528. For each Disclosure for which it is required to keep a record, Business Associate will record and maintain the information required by 45 C.F.R. § 164.528. Business Associate will maintain its record of such Disclosures for six years from the date of the Disclosure. *[NOTE FOR DRAFTING: Covered Entity is required to produce an accounting of disclosures that occurred during the six years before the date of the individual's request for an accounting, including disclosures to or by business associates of Covered Entity. If Business Associate has the ability to reproduce a list of disclosures at the time of Covered Entity's request for an accounting, Business Associate need not keep a separate record of disclosures.]*

b. Provision to Covered Entity: Within five (5) business days of receiving a notice from Covered Entity, Business Associate will provide to Covered Entity its records of Disclosures. *[NOTE FOR DRAFTING: The timeline is negotiable. Covered Entity must respond to an individual request for an accounting within 60 days.]*

c. Request by Individual: If an Individual requests an accounting of Disclosures directly from Business Associate, Business Associate will forward the request and its record of Disclosures to Covered Entity within five (5) business days of Business Associate's receipt of the Individual's request. Covered Entity will be responsible for preparing and delivering the accounting to the Individual. Business Associate will not provide an accounting of its Disclosures directly to any Individual, unless directed by Covered Entity

to do so. *[NOTE FOR DRAFTING: The timeline is negotiable. Covered Entity must respond to an individual request for an accounting within 60 days.]*

8. ACCESS TO BOOKS AND RECORDS

Business Associate will make its internal practices, books and records on the Use and Disclosure of PHI available to the Secretary of the Department of Health and Human Services to the extent required for determining compliance with the Privacy Rule, Security Rule, or Breach Notification Rule. No attorney-client, accountant-client or other legal privilege will be deemed waived by Business Associate or Covered Entity as a result of this Section. *[NOTE FOR DRAFTING: This provision related to not waiving the privilege is not required by the regulations, but is wise to include.]*

9. TERMINATION

Covered Entity may terminate this BAA upon material breach of this BAA. Covered Entity will provide Business Associate with written notice of the breach of this BAA and afford Business Associate the opportunity to cure the breach to the satisfaction of Covered Entity within thirty (30) calendar days of the date of such notice. If Business Associate fails to timely cure the breach, as determined by Covered Entity in its sole discretion, Covered Entity may terminate this BAA. This BAA otherwise terminates *[insert termination date or event]*.

10. RETURN OR DESTRUCTION OF PROTECTED HEALTH INFORMATION

a. Return or Destruction of PHI: Within thirty (30) calendar days of termination of this BAA, Business Associate will return to Covered Entity all PHI that Business Associate or its Subcontractors maintain in any form or format. Alternatively, Business Associate may, upon Covered Entity's consent, destroy all such PHI and provide written documentation of such destruction.

b. Retention of PHI if Return or Destruction is Infeasible: If Business Associate believes that returning or destroying PHI at the termination of this BAA is infeasible, it will provide written notice to Covered Entity within thirty (30) calendar days of the effective date of termination of this BAA. Such notice will set forth the circumstances that Business Associate believes makes the return or destruction of PHI infeasible and the measures that Business Associate will take for assuring the continued confidentiality and security of the PHI. Business Associate will extend all protections, limitations and restrictions of this BAA to Business Associate's Use or Disclosure of PHI retained after termination of this BAA and will limit further Uses or Disclosures to those purposes that make the return or destruction of the PHI infeasible. *[NOTE FOR DRAFTING: The timelines in both provisions are negotiable.]*

11. MISCELLANEOUS

[NOTE FOR DRAFTING: These miscellaneous provisions are not required by the regulations, but are good to have in a contract. The user should confirm that they are not in conflict any other underlying agreement(s) between the Parties.]

a. Compliance with Laws: The Parties are required to comply with federal and state laws. If this BAA must be amended to secure such compliance, the parties will meet in good faith to agree upon such amendments. If the Parties cannot agree upon such amendments, then either Party may terminate this BAA upon thirty (30) calendar days' written notice to the other Party.

b. Construction of Terms: The terms of this BAA will be construed in light of any applicable interpretation or guidance on the Privacy Rule, Security Rule or Breach Notification Rule issued by HHS.

c. No Third Party Beneficiaries: Nothing in this BAA will confer upon any person other than the Parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

d. Notices: All notices required under the BAA will be given in writing and will be delivered by (1) personal service, (2) first class mail, or (3) messenger or courier. All notices shall be addressed and delivered to the contact designated in the signature block, or other address provided by the party from time to time in writing to the other party. Notices given by mail will be deemed for all purposes to have been given forty-eight (48) hours after deposit with the United States Postal Service. Notices delivered by any other authorized means will be deemed to have been given upon actual delivery.

e. Entire Agreement: This BAA constitutes the entire agreement between the parties with regard to the Privacy Rule, Security Rule and Breach Notification Rule, there are no understandings or agreements

relating to this BAA that are not fully expressed in this BAA and no change, waiver or discharge of obligations arising under this BAA will be valid unless in writing and executed by the Party against whom such change, waiver or discharge is sought to be enforced.

f. Counterparts and Signature: This BAA may be executed in two or more counterparts, each of which shall be deemed an original and when taken together shall constitute one agreement. Facsimile and electronic signatures shall be deemed to be original signatures for all purposes of this BAA.

g. Choice of Law and Forum: The validity, construction and effect of this BAA will be governed by the laws of *[INSERT]*, without giving effect to that state's conflict of laws rules. Any Dispute will be resolved in a forum located in the *[INSERT]*.

BUSINESS ASSOCIATE	**COVERED ENTITY**
By:_____	By:_____
Print Name:_____	Print Name:_____
Title:_____	Title:_____
Date:_____	Date:_____

Contacts for Notices under this BAA:

Print Name:_____	Print Name:_____
Title:_____	Title:_____
Address:_____	Address:_____
_____	_____
_____	_____
Phone:_____	Phone:_____

